



February 26, 2015
Via ECFS Filing

Ms. Marlene H. Dortch, Secretary
Federal Communications Commission
9300 East Hampton Drive
Capitol Heights, MD 20743

RE: First Step Internet, LLC
EB Docket No. 06-36; CY2014

Dear Ms. Dortch:

Attached for filing is the Calendar Year 2014 CPNI Compliance Certification and Statement of CPNI Procedures and Compliance as required by 47 C.F.R. Section 64.2009 (e) submitted on behalf of First Step Internet, LLC.

Any questions you may have regarding this filing should be directed to my attention at 407-740-3031 or via email to sthomas@tminc.com. Thank you for your assistance in this matter.

Sincerely,

/s/Sharon Thomas

Sharon Thomas

Consultant to First Step Internet, LLC

cc: Nathan Anderson, First Step
file: First Step - FCC - Other
tms: FCx1501

Enclosures
ST/im

**ANNUAL 47 C.F.R. § 64.2009(e) OFFICER'S CERTIFICATION OF
CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI) COMPLIANCE**

EB Docket 06-36

| | |
|---|---------------------------------------|
| Annual 64.2009(e) CPNI Certification: | Covering calendar year 2014 |
| Name of company(s) covered by this certification: | First Step Internet, LLC |
| Form 499 Filer ID: | 829017 |
| Name of signatory: | Kevin Owen |
| Title of signatory: | President and Chief Executive Officer |

1. I, Kevin Owen, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. §64.2001 *et seq.*
2. Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in §64.2001 *et seq.* of the Commission's rules.
3. The company has not taken actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.
4. The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.
5. The company represents and warrants that the above certification is consistent with 47 C.F.R. §1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.



Kevin Owen, President and Chief Executive Officer

02/25/2015

Date

Attachments: Accompanying Statement explaining CPNI procedures

First Step Internet, LLC
Statement of CPNI Procedures and Compliance

First Step Internet, LLC ("FSI") does not use or permit access to CPNI to market any services outside of the total service approach as specified in 47 CFR §64.2005. FSI does not engage in marketing campaigns that would require customer approval for use of CPNI nor does it contract out any of its marketing to third parties. Other than for the direct purpose of serving the customer, no access to CPNI or customer data is authorized to any of FSI's staff, and improper access and use/abuse of CPNI by staff is grounds for immediate termination

FSI maintains a record of all sales and marketing campaigns that use CPNI.

If FSI elects in the future to use CPNI in a manner that does require customer approval, it will follow the applicable rules set forth in 47 CFR Subpart U, including the institution of operational procedures to ensure that notification is provided and customer approval is obtained before CPNI is used or disclosed.

FSI has put into place processes to safeguard its customers' CPNI, including call detail information, from improper use or disclosure by employees; and to discover and protect against attempts by third parties to gain unauthorized access to customer CPNI, as set forth below.

FSI has instituted authentication procedures to safeguard the disclosure of call detail over the telephone and online. FSI's authentication procedures do not require the use of readily available biographical information or account information as defined by the FCC. Passwords are always established with the customer at the time the account is opened; postponing password choice/not having one initially is not an option for the customer. If the customer chooses not to come up with a password, a secure password will be generated at random and issued to the customer.

Passwords on FSI's system are not just used to authenticate the user to our personnel when interacting with customer service, but are also an integral part of FSI's service itself as our computer systems require that the customer (or the customer's equipment) supply the correct password before service is rendered; thus, customers cannot make effective use of the service without knowing their password. This is true across the entire range of services FSI provides, including telephony. FSI does not disclose call detail over the telephone or online if the appropriate password is not provided.

FSI has established back-up authentication procedures for lost or stolen passwords that do not prompt the customer for readily available biographical information or account information. Company's back-up authentication procedure operates as follows: If a customer loses or forgets their password, FSI will allow them to create a new one after they have established to FSI's satisfaction that they are the owner of the account by either (a) answering if FSI calls them back at one of their phone numbers of record, or (b) the customer comes to FSI's offices in person and provides government-issued photo identification.

If the customer cannot provide a password and is not re-authenticated, FSI would only provide call detail by sending it to the customer's address of record or by calling the customer's telephone number of record.

FSI discloses CPNI at its retail location only if the customer presents a valid photo ID matching his/her account information.

FSI has procedures in place to notify customers whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed without revealing the changed information or sending the notification to the new account information. Specifically, the customer is sent an e-mail to their e-mail address of record notifying them, without specifically listing the changed information, that a change has been made to their account, and that if the change was not performed or authorized by them, they should contact the company immediately.

FSI has in place procedures to notify law enforcement in the event of a breach of customers' CPNI and to ensure that customers are not notified of the breach before the time period set forth in the FCC's rules, or, if applicable, when so authorized by law enforcement. Specifically, as soon as practicable, and in no case later than seven business days upon learning of a breach, the company will notify the U.S. Secret Service and the FBI by electronic means, as required by FCC regulations. The company will not notify customers or disclose a breach to the public until seven full business days have passed after notification to the U.S. Secret Service and the FBI, unless it believes there is an extraordinarily urgent need to notify customers before seven days in order to avoid immediate and irreparable harm. In that instance, it will only notify such customers *after* consultation with the relevant investigating agency and will cooperate with the agency's request to minimize any adverse effects of the customer notification. If the Company receives no response from law enforcement after the seventh full business day, it will promptly proceed to inform the customers whose CPNI was disclosed of the breach. The company will delay notification to customers or the public if requested to do so by the U.S. Secret Service or FBI. Notifications to law enforcement and customers are handled by a designated supervisor level employee responsible for managing the company's CPNI compliance.

FSI has not had any breaches, but does have a process in place to maintain records of all breaches discovered and notifications made to the USSS and the FBI, and to customers.

FSI has not taken any actions against data brokers in the last year.

FSI did not receive any customer complaints about the unauthorized release of CPNI or the unauthorized disclosure of CPNI in calendar year 2014.

FSI has not developed any information with respect to the processes pretexters are using to attempt to access CPNI.